AFRL-RI-RS-TR-2009-95
In-House Final Technical Report
April 2009

2-PLAYER GAME WITH UNCERTAINTY TO PROTECT MISSION CRITICAL INFORMATION OVER BLUE NETWORKS

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2009-95 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/

DAVID L. BIBIGHAUS, Maj., USAF
Chief, Cyber Defense Branch

/s/

WARREN H. DEBANY, JR.
Technical Advisor, Information Grid Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
APR 09

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
May 08 – Sep 08

4. TITLE AND SUBTITLE

2-PLAYER GAME WITH UNCERTAINTY TO PROTECT MISSION CRITICAL INFORMATION OVER BLUE NETWORKS

5a. CONTRACT NUMBER
In-House

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Sarah L. Muccio
Claire Maxey
Jennifer Nash

5d. PROJECT NUMBER
231G

5e. TASK NUMBER
IH

5f. WORK UNIT NUMBER
03

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

AFRL/RIGA
525 Brooks Rd.
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIGA
525 Brooks Rd.
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2009-95

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# 88ABW-2009-1208

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This project uses game theory to develop a non-cooperative game with a defender and an intruder. The defender attempts to protect critical information on his system using the available resources efficiently while the intruder seeks to obtain that information without being detected by the defender. This defender will defend using a different combination of only three defensive resources: encryption, distributed data, and fake honeypots. By quantifying each defense, a cost function was developed to analyze the deployment of the defenses. MATLAB is used to optimize a cost function in order to create probability distributions to determine the best possible combination of defenses to use.

15. SUBJECT TERMS
Game theory, non-cooperative, insider threat

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Sarah L. Muccio
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER (*Include area code)***
U	U	U	UU	21	N/A

TABLE OF CONTENTS

List of Tables

1 SUMMARY

In the course of executing strategic cyber defense, conducting information assurance is a crucial step in protecting our blue assets. A dynamic non-cooperative 2-player game can be formulated. The defender's goal is to protect his data while the attacker seeks to stealthily obtain the data. The defender has a limited amount of resources with which to protect his information. Each of his capabilities uses varying amounts of his resources to varying degrees of effectiveness. To maintain the scope of this project only three defensive capabilities are considered: encryption, distributed data, and fake honeypots. Meanwhile, the attacker seeks to remain undetected while gathering sensitive data. Simple deterministic strategies are easily defeated. Hence for success, the players must introduce uncertainty to disguise their intentions and confuse their opponent. Additionally in the cyber domain, layering multiple capabilities is a realistic possibility. Mathematically, the game would be carried out over the spaces of probability measures. Solutions in the form of probability distributions would indicate the optimal method to deploy defensive capabilities.

2 INTRODUCTION

Our challenge in this constantly changing world of cyber space is to shift from reactive to proactive defenses. When we approach defense in a reactionary manner we are allowing the attacker to control the conflict. This has the potential to place us in situations where our mission would be vulnerable to compromise. We are looking toward the future of cyber warfare where we instead strive to conduct cyber defense in a goal oriented, effects based manner. This important challenge requires us to approach defense strategically. We must efficiently utilize our limited defensive resources. We can accomplish this by optimizing the allocation of defensive measures on specific mission critical data. The output of our 2 player game will describe the optimal deployment of defenses on our network using probability distributions. We will maintain our flexibility by allowing the defenses to be adjusted as more knowledge is obtained about an attacker. This type of dynamic response will help us intelligently tip the odds in the defender's favor.

2.1 Technical Background

In previous work, we see Lye and Wing [8] presented a stochastic 2 player game. They recognized that probabilities were needed for realistic state transitions. However, the model was designed around reactionary defenses. There was no strategic plan for protecting the data from being compromised. The defender took action to do damage control only after successful attacks were completed. They allowed the intruder to make all of the controlling moves.

Meanwhile in the kinetic world, I previously developed a method for optimally deploying missiles with appropriate protective coverings [4]. In this case, a missile could detect which frequencies the interrogator was using. The missile could then adjust the properties of the coating to enhance stealth while in-flight. Using several of Von Neumann's theorems, I showed that the mathematical techniques used hold true even outside the confines of that kinetic project. This gives us the ability to leverage this work. However, the mapping of the kinetic world to the cyber domain is not always one to one. In addition to covering data with a single defense, we must now account for layered defenses. Failure to consider these factors could result in unrealistic solutions. There are a number of defensive measures that would not work concurrently, possibly even working against each other.

We outline below a dynamic model which will solve for the optimal method of allocating a network’s defenses. This model will also maintain the optimal configuration of a network’s defense by updating in real time as intelligence is gathered during an attack.

Today we have many defensive measures available that can be deployed strategically. To maintain the scope of this project we will only consider the following three:

- Encryption
- Distributed Data
- Fake Honeypots

We have chosen these in particular for their varying degrees of resource expense and ability to provide learning opportunities. Encryption will protect data even if it is seen. Distributed data will protect the overall picture if only a small number of the distributed data stores are compromised. Fake honeypots will create the illusion of a recognizable honeypot around real data. This will lead attackers to believe the true data is a trap and should thus be avoided [9]. The goal of this project is not just to create ways of deploying these defenses, but to devise a flexible model that will allow users to customize their defenses.

2.2 Research Outline

We must efficiently deploy our available defenses to protect mission critical data on blue networks. Solutions would be configurations of defender capabilities. These would take the form of probability distributions describing which defensive measures the defender should utilize for each of the assets listed. The goal of the defender is to protect the data and make the intruder as vulnerable to scrutiny as possible. The attacker wants to minimize the amount of intelligence that is revealed while obtaining the maximum amount of data from the defender’s system.

The defender will have a fixed amount of resources and assets to protect. We will define a metric of defenses. Classifying them as such:

- Encryption: little drain on resources, little opportunity to observe attacker.
- Distributed Data: more resources needed, increased opportunity to observe attacker.
- Fake Honeypot: significant resources, ample opportunity to observe attacker.

We created a cost function that will take the quantified values associated with these defenses as inputs. The key portion of this is not discovering the perfect metric for quantifying the defenses, rather providing the appropriate framework for using the values. This will allow the cost function to remain viable for different sets of defensive inputs in the future.

Our defender will assign some initial probability distribution of the assets targeted by the attacker. The defender will use this initial distribution to obtain an optimized solution. Creating MATLAB code to accomplish the optimization is computationally challenging. However, previous code written [4] was leveraged to reduce the amount of effort needed.

Applying defenses appropriately will present the greatest technical challenge. In the cyber domain it is possible to use multiple levels of defenses to protect mission critical data. However, not all defenses are compatible. To account for these conflicts, we must appropriately define which methods will realistically work together to provide enhanced security. We plan to accomplish this by associating variable costs with each defense. For example when we apply encryption on a particular asset, it makes it slightly more expensive to also use distributed data storage. However, even more resources would be required to also make it a fake honey pot. Accounting for compatibility issues such as these would prevent meaningless solution schemes being presented. On a separate asset though, the defensive costs might be different as various combinations are deployed.

3 METHODS, ASSUMPTIONS, AND PROCEDURES

Game theory is used to create a two player game with uncertainty to find the optimal point to gain the most valuable knowledge in order to protect critical mission information of our network. MATLAB is used to optimize the equations given in the project. By watching the intruder we will determine how much the intruder is willing to risk.

3.1 Parameter Assumptions

We start with the knowledge of the standard computer system based on the AFRL's standard desktop system. We will consider the processor, RAM, Hard Drive, and how much remains free. The standard AFRL desktop has Windows XP Professional, Processor 2.3 gigahertz, RAM of 2 gigabytes, and Hard Drive of 160 gigabytes. To help understand if any penalty will be assigned if the defenses take up to much space on the RAM and Hard Drive, a table was constructed to show how much space was taken up. (See Table 1)

If the computer constantly accesses or responds slowly then it accesses the Hard Drive when the RAM is unavailable, used up. The RAM is short term memory storage or primary storage and is resets itself on reboot of the computer system. The Hard Drive is more for long term memory or secondary storage. The time to access the RAM, measured in nanoseconds, is 200 nanoseconds. The time to access the Hard Drive, measured in milliseconds, is 12,000,000 ns or 12 milliseconds which makes the RAM 60,000 times faster to access than accessing the Hard Drive.

Table 1 Amount of Resources Required

Applications & Defenses	Computer and Processor*	Memory*	Hard Drive*
Operating System Windows XP Professional	300MHz or higher	64MB	1.5G
Internet Explorer 7th ed.	233MHz	128MB	12MB
Microsoft Office Suite 2007 (Professional)	500MHz	256MB	2G
Steganos Privacy Suite Encryption	500MHz	256MB	100MB or more available
Eclipse	233MHz	512MB	700MB
JAVA 6	166MHz	64MB	98MB
Key Focus Sensor Honeypot	1.5 GHz	512MB	500MB
Distributed Data Pastry	JAVA	LANGUAGE	
Protected Information			30% Cushion

Table 2 shows how much space will be used. The desktop will be brand new and we will assume that applications will be running during the time the defenses are running. In the future we will be able to see the incidences that will show when the penalty will be applied. Applications used are Microsoft Office Suite 2007, Internet Explorer seventh edition, eclipse, and JAVA 6. Eclipse is a software platform comprising extensible application frameworks, tools and a runtime library for software development and management. It is written primarily in Java to provide software developers and administrators an integrated development environment. Eclipse is to help the distributed data defense, Pastry, run. JAVA 6 is an added plug-in that helps Eclipse software. There are many defenses that can be used to help alongside this project but the three that will help in finding the optimal point is Encryption, Distributed Data, and Honeypots. To go further there is a type of software for each defense to be used.

- Encryption : Steganos Privacy Suite 2008
- Honeypots : Key Focus Sensor
- Distributed Data: Pastry

Table 2 Domain Expert Analysis

In Gigabytes	Resources of Hard Drive	Resources of RAM	∑ of RAM & Hard Drive	Time	Knowledge Gained
Encryption	.097	.25	.347	Best Time	Least Knowledge
Distributed Data	Eclipse .683 JAVA .095	Eclipse .5 JAVA .0625	1.3405	Neutral	Neutral
Honeypot	.488	.5	.988	Worst Time	Greatest Knowledge

3.2 Cost Function Discussion

The cost function is used to determine the optimum combination of defenses to use. The function accounts for the cost in terms of computer resources, $d,$ and the knowledge gained about the intruder by the defender,k, as well as the risk, $r,$ to the intruder as the mission information is gained, g. The computer resources we considered are hard drive, RAM, and processor speeds. For the RAM we simply added up the amount of RAM recommended for the three defenses and the RAM used by other common applications. We determined that if that sum exceeded the total RAM available on the computer than there would be a penalty as virtual memory was created in the hard drive to accommodate the overflow.

There was then a term added for the penalty of overflowing the RAM and forcing the hard drive to be accessed. For the hard drive we decided that we would leave at least thirty percent free for actual mission requirements. We made that reduced amount the maximum available. Then we added the recommended amount of hard drive for the commonly used applications and the defenses to be deployed. Additionally, we took into account the overflow from the RAM if it was exceeded. For the knowledge gained by the defender/risk of discovery to the intruder portion we used domain experts to evaluate the defenses on a scale of 1-10. Table 3 was made which included all of the combinations in which the defenses could be deployed; each by itself, different pairs, and all together. The hard drive and RAM requirement for each different way were added together and then associated with an index that will be used in the determination of the knowledge/risk portion of the equation.

Table 3 Defensive Combinations

Defenses	Resources Used (Hard Drive & RAM)	Defender's Knowledge
A	.3470	1
B	1.3405	2
C	3.9520	4
A+B	1.6875	2
B+C	5.2925	6
A+C	4.2990	5
A+B+C	5.6395	6

While A, B, and C can represent any type of defense, for this project A is encryption, B is distributed data, and C is honeypots. We chose to factor in the resources it would take to deploy four honeypots on each node.

In front of each part of the equation we added a constant so that each term (RAM usage, RAM overflow, hard drive usage, and knowledge/risk) could be weighted independently of one another depending on which factor is most important to the defender.

It was determined that the processor speed would not be a factor to consider in the cost equation as the speed of the processor being used by the computer we chose exceeded the recommended minimum requirement for each of the defenses to be used. The minimum recommendations take into account that other software will be running at the same time as the defenses and so the processor speed is not a limiting factor.

Hard Drive →(Sum of Applications) + (Sum of Defenses) + (RAM overflow) < .7*(hard drive size)

RAM → (Sum of Applications) + (Sum of Defenses) = RAM used
If (RAM used) > (RAM size), then (RAM used) = (RAM size) and
(RAM overflow) = (RAM used) – (RAM size)

The cost function we derived with is as follows where μ, ε, $w_{1,}$ and w_2 are the weighting constants. The constant ***p*** is the penalty for overflowing the RAM. *Hard Drive used* and *RAM used* are the sums of each respective resource that the applications and defenses are using. *RAM overflow* is the amount the RAM size has been exceeded by. The *Defender's Knowledge* term that takes into account the knowledge the defender gains about the intruder while the *Intruder's Risk* term shows how willing the intruder is to risk detection. [2].

Cost = μ (Defenses) + ε (Defender's Knowledge) + p (RAM overflow) +
w_1 (Intruder's Risk) -w_2 (Mission Information lost)

For our simulations, we let all weighting constants equal one. However, should domain experts/operators feel that one or more variable is of greater consequence, this can be adjusted.

3.3 Mathematical Formulation

Here is a brief of the background equations that is projected is based upon. For a full derivation please see [4]

Defender: Uses parameters defenses and knowledge gained $(d, k) \in D \times K$
Intruder: Uses parameters risk of discovery and advantaged gained $(r, g) \in R \times G$

This leads us to the following probability distributions:

$$P_e\,(d, k) = \; P_e^1(d)P_e^2(k) over\; D \times K$$

$$P_i\,(r, g) = \; P_i^1(r)P_i^2(g) over\; R \times G$$

For $P_e \in \; \mathcal{P}(D \times K), P_i \in \mathcal{P}(R \times G)$, define

$$J(P_e, P_i) = \int_{D\times K}\int_{R\times G} |C(d, k, r, g)|^2 \; dP_e\,(d, k)\; dP_i\,(r, g)$$

Goal: Find $P_e{}^* \in \; \mathcal{P}(D \times K), P_i{}^* \in \mathcal{P}(R \times G)$ such that

$$J(P_e{}^*, P_i{}^*) = \max_{\mathcal{P}(D\times K)} \min_{\mathcal{P}(R\times G)} J(P_e, P_i)$$

Upper and Lower values of the game: $(\overline{J} \geq \underline{J}\,)$

- $\overline{J} = \sup_{\mathcal{P}(D\times K)} \inf_{\mathcal{P}(R\times G)} J(P_e, P_i)$ security level for defender
- $\underline{J} = \inf_{\mathcal{P}(R\times G)} \sup_{\mathcal{P}(D\times K)} J(P_e, P_i)$ security level for intruder

If $J^* = \overline{J} = \underline{J}$, then J^* is the optimal cost of the game.

If there exists $(P_e{}^*, P_i{}^*)$such that

$$J^* = J(P_e{}^*, P_i{}^*)$$

then $(P_e{}^*, P_i{}^*)$ is called the saddle point solution of the game.

Von Neumman's Theorem:

Suppose X_0 , Y_0 are compact, convex subsets of metric linear spaces X, Y respectively. Further suppose that

- for all $y \in Y_0$, $x \rightarrow f\ (x, y)$ is convex and lower semi continuous;
- for all $x \in X_0$, $y \rightarrow f\ (x, y)$ is concave and upper semi continuous.

Then there exists a saddle point (x^*, y^*) such that

$$f(x^*, y^*) = \max_{X_0} \min_{Y_0} f\ (x, y)$$

Theorem:

Suppose D, K, R, G are compact and the spaces $X_0 = \mathcal{P}(D \times K)$,
$Y_0 = \mathcal{P}(R \times G)$ are taken with the Prohorov metric.
Then X_0 , Y_0 are compact, convex subsets of $X \quad = C_B^*(D \times K)$, and
$Y \quad = C_B^*(R \times G)$ respectively.
Moreover, there exists $({P_e}^*, {P_i}^*) \in \mathcal{P}(D \times K) \times \mathcal{P}(R \times G)$ such that

$$J({P_e}^*, {P_i}^*) = \max_{\mathcal{P}(D \times K)} \min_{\mathcal{P}(R \times G)} J(P_e, P_i)$$

To illustrate the computational framework, take

$$dP_e^M\ (d, k) = \sum_{m=1}^{M} p_m^M\ \delta_{(d_m^M, k_m^M)}\ dd\ dk \leftrightarrow \overline{p}^M = \{p_m^M\}_{m=1}^M \in \boldsymbol{P^M} \approx\in \mathcal{P}(D \times K)$$

$$dP_i^N\ (r, g) = \sum_{n=1}^{N} p_n^N\ \delta_{(r_n^N, g_n^N)}\ dr\ dg \leftrightarrow \overline{q}^N = \{q_n^N\}_{n=1}^N \in \boldsymbol{Q^N} \approx\in \mathcal{P}(R \times G)$$

where here '≈' represents approximation in the Prohorov metric.
Then $J(P_e^M, P_i^N)$ reduces to

$$\mathcal{J}\left(\overline{p}^M, \overline{q}^N\right) = \sum_{m=1}^{M} \sum_{n=1}^{N} p_m^M\ |C(d_m, k_m, r_n, g_n)|^2 p_n^N$$

where C is the cost function derived earlier. Since $\boldsymbol{P^M}$, $\boldsymbol{Q^N}$ are compact, convex subsets of C^M, C^Nrespectively, we have the following theorem.

Theorem:

For fixed M, N there exists$\left(\overline{p}_*^M, \overline{q}_*^N\right)$
in $P^M \times Q^N$, such that

$$\mathcal{J}^* = \mathcal{J}\left(\overline{p}^M, \overline{q}^N\right) = \max_{\overline{p}^M \in P^M} \min_{\overline{q}^M \in Q^M} \mathcal{J}\left(\overline{p}^M, \overline{q}^N\right)$$

$$\mathcal{J}^* = \mathcal{J}\left(\overline{p}^M, \overline{q}^N\right) = \max_{\overline{p}^M \in P^M} \min_{\overline{q}^M \in Q^M} \mathcal{J}\left(\overline{p}^M, \overline{q}^N\right)$$

$$= \min_{\overline{q}^M \in Q^M} \max_{\overline{p}^M \in P^M} \mathcal{J}\left(\overline{p}^M, \overline{q}^N\right)$$

Assume further that $(d, k, r, g\ ) \rightarrow C(d, k, r, g)$ is continuous on $D \times K \times R \times G$ which is assumed compact. Then there exists a sequence $\left(\overline{p}_*^{M_m}, \overline{q}_*^{N_n}\right)$ with corresponding $(\boldsymbol{P}_{\boldsymbol{e}}^{\boldsymbol{M_m}}, \boldsymbol{Q}_{\boldsymbol{i}}^{\boldsymbol{N_n}})$ converging in the Prohorov metric to (P_e^*, Q_i^*) which is a saddle point for the original Min Max problem.

4 DISCUSSION OF RESULTS

We carried out a number of different optimization trials using these defenses outlined above. We present in Table 4 a sample of results obtained for the case with all available combinations of defenses. The min max calculations are readily carried out using standard MATLAB minimization packages. These results show that about 65% of the computers in our network should be equipped with the defensive combination of A, B, and C. While the other 35% should have only B and C. Meanwhile the intruder is extremely risk averse with these strong defenses in place. (See Figure 1).

Table 4 Results with all Defenses

Defenses	Resources Used (Hard Drive & RAM)	Defender's Knowledge	Probabilities
A	.3470	1	**1.1045e-022**
B	1.3405	2	**-1.2448e-017**
C	3.9520	4	**-7.7845e-024**
A+B	1.6875	2	**-7.7845e-024**
B+C	5.2925	6	**3.5255e-001**
A+C	4.2990	5	**-2.0596e-022**
A+B+C	5.6395	6	**6.4745e-001**

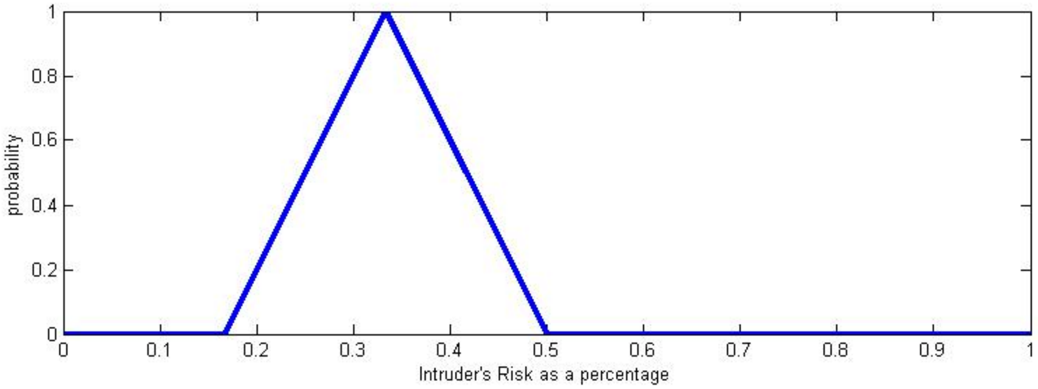

Figure 1 Intuder's Risk

Next we limit the defender to only have defenses A and B. This takes away the most powerful defense that the defender relied on in the previous case. Now the results show that the optimal deployment of defenses is to have 60% with A and B while the remaining 40% only require A. (See Table 5) Meanwhile this allows our intruder to become much more bold. The intruder is more likely to take more risks. (See Figure 2)

Table 5 Results without Defense C

Defenses	Resources Used (Hard Drive & RAM)	Defender's Knowledge	Probabilities
A	.3470	1	**3.9678e-001**
B	1.3405	2	**0**
A+B	1.6875	2	**6.0322e-001**

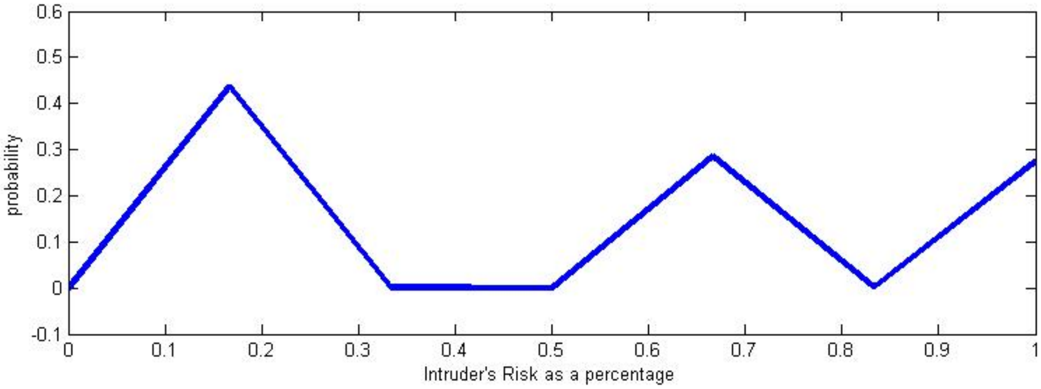

Figure 2 Intruder's Risk

5 CONCLUSIONS

The end result of this project will be the determination of the best way to deploy defenses on a system. By using MATLAB to optimize the cost function, we created probability distributions that showed what the best combination of defenses to use is when there is uncertainty in how and when the intruder will attempt to gain entry. By ‘best defenses’ we want the ones that use few resources (RAM and hard drive) while still allowing the defender to efficiently gain the most knowledge about the intruder before the intruder discovers they are being observed and gets out as well as protect the mission information. The resulting work is flexible enough to allow for a variety of different defenses to work together to protect the network. Each variation can be fit into the overall picture of our network protection.

6 FUTURE WORK

Future work also includes monitoring the environment to determine when an intruder enters and updating the optimization to alter the defenses in a way most beneficial to the defender in terms of protecting critical information and not wasting resources in the process. When an intruder is detected, the initial probability distribution of the assets targeted by the attacker will be updated. The defender will seek an updated optimization. This continual process will give the defender the opportunity to reinforce the defenses without wasting resources.

7 REFERENCES

1. Banks, HT and Kunisch, K, *Estimation Techniques for Distributed Parameter Systems*, Birkhauser, Boston, 1989.
2. Billingsley, P, *Convergence of Probability Measures*, John Wiley, New York, 1968.
3. Colton, D and Kress, R, *Inverse Acoustic and Electromagnetic Scattering Theory*, Vol. 93 of Applied Mathematical Sciences, Springer-Verlag, Berlin, 2nd ed., 1998.
4. Grove. S, Optimization Problems in the Presence of Uncertainty, *Ph.D. dissertation, North Carolina State University*, 2007.
5. Hamilton, S. Miller, W., Ott, A., and Saydjari, O., Challenges in Applying Game Theory to the Domain of Information Warfare, *The Information Survivability Workshop*, 2001
6. Hamilton, S. Miller, W., Ott, A., and Saydjari, O., The Role of Game Theory in Information Warfare, *The Information Survivability Workshop*, 2001
7. Huber, PJ, *Robust Statistics,* Wiley & Sons, New York, 1981.
8. Lye, K. and Wing, J.M., Game strategies in network security. *Proceedings of the 2002 IEEE Computer Security Foundations Workshop*, 2002
9. Rowe, N., Duong, B., and Custy, E., Fake Honeypots: A Defensive Tactic for Cyberspace, *Proceeding of IEEE Workshop on Information Assurance*, 2006
10. von Neumann, J, Zur theorie der gesellschaftsspiele. *Math. Ann.*, **100** (1928), 295–320.
11. von Neumann, J and Morgenstern, O, *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, NJ, 1944.
12. Yu, V. Prohorov, Convergence of random processes and limit theorems in probability theory, *Theory. Prob. Appl.*, **1** (1956), 157–214.